委託先事業者等公開用抜粋版

情報セキュリティ対策基準

【留意事項】

本基準（委託先事業者等公開用抜粋版）は、区における情報システム構築等の外部委託案件に関し、情報セキュリティ対策の側面から外部委託事業者が遵守すべき内容を示すものである。

文中には、「情報システム管理者は」というように職員が主語となっている内容であっても、実質的には「外部委託事業者に伝達のうえ情報システムに実装させることにより遵守すべき事項」等が存在する。

以上を踏まえ、情報システム構築等の受託者においては、当該受託事案と関連のある記載事項全てを考慮した情報セキュリティ対策を講じること。

施行日：平成 24 年 11 月 21 日

世田谷区

改訂履歴

年月日	版番号	改訂理由・内容
平成 24 年 11 月 21 日	1.1	初版発行
平成 28 年 1 月 1 日	1.2	ポリシー改定を反映
平成 31 年 4 月 1 日	1.3	情報セキュリティ対策基準改定を反映
令和 2 年 4 月 1 日	1.4	情報セキュリティ対策基準改定を反映

目次

１　目的

本対策基準は、基本方針に定める情報セキュリティを確保するために遵守するべき行為及び判断等の基準を定め、情報資産を適切に取扱うことにより、安定的かつ継続的な行政サービスの提供を維持することを目的とする。

２　省略

３　適用範囲

⑴行政機関の範囲

対策基準が適用される行政機関は、区長部局、行政委員会、議会事務局とする。

これらの対象行政機関で、情報資産に接する全ての者（職員（会計年度任用職員を含む。）並びに外部委託事業者等をいう。以下「職員等」という。）

⑵情報資産の範囲

本対策基準が対象とする情報資産は次のとおりとする。(ただし、教育委員会における学校教育に用いるものを除く。)

・ネットワーク、情報システム及びこれらに関する設備や設置場所
・ネットワーク及び情報システムで取り扱う情報（これらを印刷したものを含む。）や電磁的記録媒体
・情報システムの仕様書及びネットワーク図等のシステム関連文書

情報資産の種類	情報資産の例
ネットワーク	通信回線、通信ケーブル、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル
電磁的記録媒体	サーバ、端末、通信機器等に内蔵される電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

４　省略

５　省略

６　情報システム全体の強靭性の向上

(1) マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(IP アドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。

イ　情報のアクセス及び持ち出しにおける対策

①情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。

②情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(2)LGWAN 接続系

ア　LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

①インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送する方式

②インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(3)インターネット接続系

ア　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

イ　区市町村のインターネット接続口を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や東京都等と連携しながら、

情報セキュリティ対策を推進しなければならない。

7　物理的対策

(1)機器の取付け等

情報システムは、原則として次の措置を講じた上で設置しなければならない。ただし、設置場所の制約等により設置することができない事項にあっては、CISO 補佐の指定した取扱いを行うものとする。

ア　機器の取付け

情報システムに係る装置の取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響をできる限り排除した場所に設置すると共に、施錠するなど容易に取り外すことができないような措置を講じなければならない。また、重要性の高い情報資産（重要性分類Ⅰ、Ⅱ等）を取扱うシステムは、災害時でも被害の程度が低いと想定される安全な場所に設置しなければならない。

ウ　機器の電源

①サーバ等の機器の電源については、当該機器を適正に停止するまでの間に十分な電力を供給する装置等を備え付けるように努めなければならない。

②落雷等による過電流に対してサーバ等の機器を保護するための措置を講じるように努めなければならない。

エ　通信ケーブル等の配線

①配線は、損傷や情報の傍受等を受けることがないように適正な措置を講じなければならない。

②情報化基盤管理者及び情報システム管理者は、通信ケーブル及び電源ケーブルの損傷などの報告に対して適正に対応しなければならない。

③情報化基盤管理者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置するなど適正に管理しなければならない。

④情報化基盤管理者、情報システム管理者及び契約により操作を認められた外部委託事業者等以外の者が配線を変更、追加してはならない。

8　人的対策

情報資産の人的対策は、次に掲げるところにより実施するものとする。

(7)認証情報の管理

ウ　ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければなら

ない。

①自己が利用しているIDは、他人に利用させてはならない。

②共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

エ　パスワードの管理

職員等は、自己の保有するパスワードに関して、次の事項を遵守しなければならない。

①パスワードは、他者に知られないように管理すること。

②パスワードを秘密にし、パスワードの照会等には一切応じないこと。

③パスワードのメモの不用意な作成や、端末等の本体及びその周辺へのメモの貼り付けなどにより、パスワード流出の機会を作らないこと。

④パスワードは十分な長さとし、文字列は、想像しにくいものとすること。

⑤情報システム又はパスワードに対する危険の恐れがある場合は、速やかにパスワードを変更すること。

⑥複数の情報システムを取扱う職員等は、パスワードをシステム間で共有しないこと。

⑦仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更すること。

⑧サーバ、ネットワーク機器及び端末等にパスワードを記憶させないこと。

⑨職員間でパスワードを共有しないこと。ただし、IDの共用を指定されている場合はパスワードを共有できることとするが、この場合のパスワードは定期的に変更し、パスワードを再利用しないこと。

９　技術的及び運用における対策

情報資産の技術的及び運用における管理等は、次に掲げるところにより実施するものとする。

(1)コンピュータ及びネットワークの管理

ウ　ログ及びシステム変更記録等の管理

①情報化基盤管理者及び情報システム管理者は、あらかじめ項目や保存期間等を定めて取得することとしたログ及び情報セキュリティの確保に必要な記録を全て取得し、一定期間保存しなければならない。

②情報化基盤管理者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

③情報化基盤管理者及び情報システム管理者は、定期的にログ等を分析、監視しなければならない。

④情報化基盤管理者及び情報システム管理者は、基幹システム等、特に重

要な情報を取り扱う情報システム及びネットワークについては、取得したログを定期的に点検又は分析する機能又は仕組みを設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析しなければならない。

エ　障害記録

情報化基盤管理者及び情報システム管理者は、職員等から報告のあった情報、システムの障害に対する処理及び問題等を障害記録として体系的に記録し、常に活用できるように保存しなければならない。

オ　情報システム仕様書等の管理

情報化基盤管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等については、記録媒体にかかわらず業務上必要とする者のみが閲覧できるよう、適正に保管しなければならない。

カ　バックアップ

情報化基盤管理者及び情報システム管理者は、重要性の高い情報資産を取扱うシステム等に記録された情報については、冗長化措置にかかわらず、その重要度に応じて期間を設定し、定期的にバックアップを取らなければならない。

キ　情報システムの入出力データ

①情報システムに入力されるデータは、適正なチェック等を行い、それが正確であることを確実にするための措置を講じなければならない。

②情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確保しなければならない。

タ　電子署名・暗号化

職員等は、外部に送るデータについて必要がある場合には、区で定める電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

また、区で定めた方法で暗号のための鍵を管理しなければならない。

⑵アクセス制御

ア　アクセス制御等

情報化基盤管理者及び情報システム管理者は、利用者がその権限を超えて情報システムを利用することができないように適正な措置を講じなければならない。

イ　利用者登録

①情報化基盤管理者及び情報システム管理者は、利用者の登録、変更、抹消、登録情報の管理、異動又は世田谷区外への出向等の職員等及び退職者における利用者 ID の取扱い等については、定められた方法にしたが

って適正に行わなければならない。

②情報システムのアクセスに必要な利用者登録・変更は、情報化基盤管理者又は情報システム管理者に対する申請により行う。

③職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報化基盤管理者又は情報システム管理者に通知しなければならない。

ウ　管理者権限

①情報化基盤管理者及び情報システム管理者は、管理者権限等の特権 ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

④情報化基盤管理者及び情報システム管理者は、特権 ID 及びパスワードの変更について、外部委託事業者に行わせる場合は、厳重に管理しなければならない。

⑤情報化基盤管理者及び情報システム管理者は、特権 ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

⑥情報化基盤管理者及び情報システム管理者は、特権 ID を初期設定以外のものに変更しなければならない。

オ　ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン･ログアウト時刻の表示等により、正当な権限を持つ職員等がログインしたことを確認できる仕組みがある場合、これを有効に活用しなければならない。

カ　管理者によるパスワードの管理方法

パスワードの管理方法は次に掲げるとおりとする。

①情報化基盤管理者及び情報システム管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。

②情報化基盤管理者及び情報システム管理者は、職員等のパスワードについて、定期的にその妥当性について調査を行わなければならない。

③情報化基盤管理者及び情報システム管理者は、第三者に知られることのないよう、暗号化等パスワードの取扱いに注意しなければならない。

④情報化基盤管理者及び情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させることが可能なシステムとするよう努めなければならない。

⑤情報化基盤管理者及び情報システム管理者は、認証情報の不正利用を防止するた

めの措置を講じなければならない。

キ　接続時間の制限

管理者権限によるネットワーク及び情報システムへの接続については、必要最小限の接続時間に制限しなければならない。

(3) システム開発、導入、保守等

ア　情報セキュリティ要求事項の分析及び明示

情報システム管理者は、情報システムの開発及び保守に関する情報セキュリティ要求事項を分析し、明確に定めなければならない。

イ　情報システムの調達

①情報システムの調達

(a) 情報化基盤管理者及び情報システム管理者は、システム開発、導入、保守等の調達にあたっては、一般に公開する調達に関する仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

(b) 情報化基盤管理者及び情報システム管理者は、機器及びソフトウェアを購入等する場合、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

②情報システムの受託事業者への対応

(a) 新たな情報システムの開発を外部委託事業者等に委託する場合には、導入前のセキュリティ検証要求事項等を定めなければならない。

(b) 情報システム管理者は、情報システムの受託事業者に対して名札等を着用させるとともに、必要に応じて身分証明書等の提示を求め、従事者の確認を行わなければならない。

ウ　情報システムの開発

①情報システムの開発における責任者及び作業者の特定

(a) 情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。

(b) 情報システム管理者は、システム開発案件に関するルールを定めなければならない。

②システム開発における責任者、作業者の ID の管理

(a) 情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

(b) 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

(a) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(b)情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

エ　開発と移行

①情報システム管理者は、重要なシステムについて、システム開発、保守及びテスト環境と、システム運用環境を分離しなければならない。

②情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

③情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

④情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

⑤情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

オ　テスト

①情報システム管理者は、新たにシステムを導入する際には、既に稼働しているシステムに接続する前に十分な試験を行わなければならない。

②情報システムのオペレーティングシステムやソフトウェアを変更する場合には、その手続を定め技術的なレビュー及びテストを実施し、悪影響がないことを確認しなければならない。

③情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

④情報システム管理者は、システムの最終検証等の必要やむを得ない場合を除いて、個人情報及び機密性の高い情報資産を、テストデータに使用してはならない。

⑥情報システム管理者は、開発したシステムについて受け入れテストを行う場合、システム管轄する所属と利用する所属が、それぞれ独立したテストを行わなければならない。

カ　暗号による管理策

情報化基盤管理者及び情報システム管理者は、情報の機密性を保護するため、特に取扱いに慎重を要する電子データが不正アクセスにさらされないよう、必要に応じて暗号化技術を使用するように努めなければならない。暗号化技術を使用する際には、適用される法令及び規制、適用性や管理技術を十分に調査しなければならない。

キ　機器の修理及び廃棄

①電磁的記録媒体を有する機器について、外部委託事業者等に修理又は廃棄させる場合には、情報資産が消去された状態で行わなければならない。

⑷不正プログラム対策（コンピュータウイルス対策）

ア　情報化基盤管理者および情報システム管理者の措置事項

情報化基盤管理者および情報システム管理者は、原則として次のウイルス対策を講じなければならない。

③業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないこと。

ウ　情報システム管理者の措置事項

情報システム管理者は、次の事項を遵守しなければならない。

①サーバ及びパソコンのウイルスチェックを行うこと。

②ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

③ウイルスチェック用のソフトウェアは、常に最新の状態に保つこと。

⑸不正アクセス対策

ア　情報化基盤管理者及び情報システム管理者の措置事項

情報化基盤管理者及び情報システム管理者は、次の対策を講じなければならない。

①使用終了又は使用される予定のないデータの出入口（ポート）を長期間空けた状態のままにしてはならない。

②サーバ及びクライアント上の不要な機能については、削除又は停止しなければならない。

③不正アクセスによるウェブページ書換え防止を確実にするために、データの書換え記録を保存し、情報化基盤管理者及び情報システム管理者が確認できるようにしなければならない。

⑹技術的脆弱性の管理

情報システム管理者は、情報システムの脆弱性に対し速やかに対応するために、以下の管理策を実施しなければならない。

ア　技術的脆弱性情報の取得

情報システム管理者はシステムに導入されているハードウェア及びソフトウェアに関連する技術的脆弱性情報を、各メーカー等から定期的に収集しなければならない。

イ　技術的脆弱性への対応

①情報システム管理者は技術的脆弱性情報の取得により判明した情報を、重要性、影響範囲等を基に、速やかに関係者に通知しなければならない。

②通知を受けた関係者はその指示に従い、速やかに対策を講じなければな

らない。

(7)情報システムの管理

ア　情報システムの監視

①情報セキュリティに関する事案を検知するため、情報化基盤管理者及び情報システム管理者は、常に情報システムの監視を行わなければならない。

②外部と常時接続するシステムについては、ネットワーク侵入監視装置等を設置し、監視を行わなければならない。

③上記の監視により得られた記録については、消去や改ざん等されないように適正な措置を講じ、定期的に安全な場所に保管するとともに、これらの記録の正確性を確保するため、正確な時刻の設定に努めなければならない。

ウ　委託による運用

①情報システム管理者及び情報化管理者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

１０　危機管理対策

情報資産への侵害等に対する危機管理対策については、次に掲げるところにより実施するものとする。

(1)緊急時対応計画の策定

CISO 又は情報システム推進委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合における体制、運用、証拠保全、被害拡大の防止及び復旧等の適切な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を以下のとおり定める。

ア　関係者の連絡先及び緊急時対応マニュアル

①情報化基盤管理者及び情報システム管理者は、情報システムごとに緊急連絡先名簿、緊急時対応マニュアルを整え、全ての職員等に対し緊急時の対応方法について周知しなければならない。

イ　発生した事案に係る報告すべき事項

①セキュリティに関する事案を発見した者は、次の項目について速やかに CISO 補佐に報告しなければならない。

(a)事案の状況

(b)事案が発生した原因として、想定される行為

(c)確認した被害・影響範囲（事案の種類、損害規模、復旧に要する額等）
(d)ログ等

ウ　事案への対処

③情報システム管理者は、次の事項が発生し情報資産保護のために情報システムの停止がやむを得ないと判断した場合には、情報システムを停止しなければならない。その際、情報システム管理者は、緊急時対応マニュアルに基づき対応しなければならない。

(a)コンピュータウイルス等不正プログラムが、情報資産に深刻な被害を及ぼしているとき。
(b)災害等により電源を供給することが危険又は困難なとき。
(c)その他情報資産に係る重大な被害が想定されるとき。

④情報化基盤管理者及び情報システム管理者は、事案に係るシステムのアクセス記録及び経過記録等を保存しなければならない。

⑤情報化基盤管理者及び情報システム管理者は、事案に係る証拠保全を実施するとともに、再発防止の暫定措置を講じた後、早期に復旧に努めなければなければならない。復旧後、必要と認められる期間、再発監視を行わなければならない。

１１　省略

１２　法令遵守

(1)適用法令の識別

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令や契約上の要求事項を遵守し、これに従わなければならない。

・地方公務員法（昭和２５年法律第２６１号）
・著作権法（昭和４５年法律第４８号）
・不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
・行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）
・サイバーセキュリティ基本法（平成 ２８年法律第３１号）
・世田谷区個人情報保護条例（平成４年３月規則第２号）

(2)知的所有権

著作権、意匠権、商標等の知的所有権に関わる物件の使用及びソフトウェア製品の使用許諾契約をする場合には、法的制限事項に適合するように実施しなければならない。

(3)個人情報の保護

個人情報を取扱う職員等は、情報セキュリティポリシーのほか、世田谷区個人情報保護条例（平成４年３月条例第２号）も遵守し、その定めに基づいた対策を講じなければならない。

１３　省略

１４　約款による外部サービスの利用

民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等を利用する場合には、リスクを十分踏まえた上で利用を判断し、以下のセキュリティ対策を講じるものとする。

(1)約款による外部サービスの利用に係る規定の整備

②情報化管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、重要性分類Ⅱ以上の情報が取扱われないように規定しなければならない。

ア　約款によるサービスを利用してよい範囲

イ　業務により利用する約款による外部サービス

ウ　利用手続及び運用手順

(2)約款による外部サービスの利用における対策の実施

①情報化管理者は、約款による外部サービスの利用にあたっては、あらかじめ情報化基盤管理者と協議しなければならない。

②情報化管理者は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認し、適切な措置を講じた上で利用しなければならない。

１５　省略

１６　評価・見直し

(1)監査

ア　実施方法

CISOは、情報セキュリティ監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。外部委託事業者等への監査についても同様とする。